Cryptography I, homework sheet 6

Due: 18 November 2011, 10:45

For this exercise sheet you have significantly more time than usual due to the exam break at TU/e; you can earn 20 points for this sheet. You can find more information on polynomials on p 34 ff. in the number theory and algebra script.

1. Consider the subset $\mathbb{Q}(i) \subset \mathbb{C}$ defined by
$$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}.$$
Show that $(\mathbb{Q}(i), +, \cdot)$ is a field, where addition and multiplication are defined as in $\mathbb{C}$.

2. Let $K = \mathbb{Z}/2\mathbb{Z}$ be the field of integers modulo 2. Consider the residue classes of $K[x]$ modulo $f(x) = x^n + 1$ for some positive integer n, i.e. $R = K[x]/(x^n + 1)K[x]$. Note that R can be represented as
$$R = \left\{a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \mid a_i \in K\right\}.$$
Show that R is a commutative ring with unity.

3. Let K be a field of characteristic p, where p is prime. Show that for any integer $n \geq 0$ one has
$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$
for all $a, b \in K$.
Hint: You can use the binomial theorem and use proof by induction.

4. Let K be a field and let $f(x) \in K[x]$. Show that $a \in K$ is a root of f if and only if $(x - a) | f(x)$.
Hint: divide $f(x)$ by $x - a$ and study the remainder.

5. Let $f \in K[x]$ be a polynomial. Show that if α is a multiple root of f then $(x - \alpha) | \gcd(f, f')$.
Here f' denotes the derivative of f which is defined as $f'(x) = \sum_{i=1}^{n} i f_i x^{i-1}$ for $f(x) = \sum_{i=0}^{n} f_i x^i$. The i in $i f_i x^{i-1}$ is considered modulo the characteristic of K if $\text{char}(K) > 0$. This derivative satisfies the usual rules, in particular $(gh)' = g'h + gh'$ and $(g^m)' = m g^{m-1} g'$.